Microsoft Defender capabilities disabled

One of REvil’s initial endpoint actions is to disable several Microsoft Defender for Endpoint capabilities, such as accurate time monitoring, IPS, cloud lookup, script scanning, controlled folder access, network protection, and stop cloud sample submissions. When the ransomware runs, it issues a PowerShell command to turn these all off, so if you are monitoring PowerShell scripting, you can see all of these protections being disabled concurrently. If you are not running PowerShell logging, you can still use Microsoft Sysmon or Windows Security logs to detect these commands.

Required data

- Microsoft: Windows event logs
- Microsoft: Sysmon

Procedure

Option 1 - Search using PowerShell logging

1. Add a configuration in your inputs.conf file to monitor WinEventLog://Microsoft-Windows-PowerShell/Operational on the client where your Splunk Universal Forwarder is installed.
2. Run the following search. You can optimize it by specifying an index and adjusting the time range.

```
source="WinEventLog:Microsoft-Windows-PowerShell/Operational"
| search Message="*Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend***"
| table _time, host, Message
```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>source=&quot;WinEventLog:Microsoft-Windows-PowerShell/Operational&quot;</td>
<td>Search only Windows PowerShell operational data.</td>
</tr>
<tr>
<td></td>
<td>Search for any of the defined Windows Defender capabilities being turned off in the same command line.</td>
</tr>
</tbody>
</table>

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Explanation

Searching for specific capabilities has the benefit of creating an exact match. Be aware, however, that searching for these capabilities within this search potentially risks missing variants that reorder the capabilities in the command itself. If you don’t want to search for specific capabilities, you can use replace this line with a wildcard search: `| search Message="*Set-MpPreference -Disable* $true* -Disable* $true*"` In addition, certain values can be shortened in scripts. For example, `-drtm` can be used in place of `-disablerealtimemonitoring`, so flexibility in searches is key.

Display the results in a table with columns in the order shown.

### Result

If any results indicate the infection has been detected, then the host or computer where the vulnerability is detected needs to be further investigated and remediated according to your response plan. This involves a final step of re-imaging the system with a known good system build after investigation.

### Option 2 - Search using Sysmon

1. Enter the following search command into the search bar. Depending on your configuration, the source and sourcetype might vary slightly. This same logic can be applied to your EDR platform of choice.

   ```bash
   | table _time, host
   ```

### Search explanation

Here is an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.
Splunk Search

- source="WinEventLog:Microsoft-Windows-Sysmon/Operational"
- EventCode=1
- CommandLine=*powershell.exe
- Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend*

| table _time, host

Explanation

- Search only Sysmon operational data.
- Search for a process creation event.
- Search for a powershell.exe process.
- Search for any of the defined Windows Defender capabilities being turned off in the same command line.
- Searching for specific capabilities has the benefit of creating an exact match. Be aware, however, that searching for these capabilities within this search potentially risks missing variants that reorder the capabilities in the command itself. If you don't want to search for specific capabilities, you can use replace this line with a wildcard search: | search Message="*Set-MpPreference -Disable* $true* -Disable* $true*"
In addition, certain values can be shortened in scripts. For example, -drtm can be used in place of -disablerealtimemonitoring, so flexibility in searches is key.
- Display the results in a table with columns in the order shown.

Result

If any results indicate the infection has been detected, then the host or computer where the vulnerability is detected needs to be further investigated and remediated according to your response plan. This involves a final step of reimaging the system with a known good system build after investigation.

Option 3 - Search using Windows Event Logs

1. Enter the following search command into the search bar. Depending on your configuration, the source might vary slightly.

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.

| table _time, host

**Search explanation**

Here is an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>source=&quot;WinEventLog:Security&quot;</td>
<td>Search only Windows security data.</td>
</tr>
<tr>
<td>EventCode=4688</td>
<td>Search for a process creation event.</td>
</tr>
<tr>
<td>Process_Command_Line=&quot;*powershell.exe&quot;</td>
<td>Search for a powershell.exe process.</td>
</tr>
<tr>
<td>Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend*&quot;</td>
<td>Search for any of the defined Windows Defender capabilities being turned off in the same command line. Searching for specific capabilities has the benefit of creating an exact match. Be aware, however, that searching for these capabilities within this search potentially risks missing variants that reorder the capabilities in the command itself. If you don't want to search for specific capabilities, you can use replace this line with a wildcard search:</td>
</tr>
<tr>
<td></td>
<td>In addition, certain values can be shortened in scripts. For example, -drtm can be used in place of -disablerealtimemonitoring, so flexibility in searches is key.</td>
</tr>
<tr>
<td></td>
<td>Display the results in a table with columns in the order shown.</td>
</tr>
</tbody>
</table>

**Result**

If any results indicate the infection has been detected, then the host or computer where the vulnerability is detected...
needs to be further investigated and remediated according to your response plan. This involves a final step of re-imaging the system with a known good system build after investigation.

**Next steps**

You might be interested in other processes associated with the Detecting REvil ransomware infections use case.